|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

**ЛЕКЦИОННЫЕ МАТЕРИАЛЫ**

|  |  |
| --- | --- |
| **Б2.В,ДВ.3.1 «Криптографические методы защиты информации 11504»** | |
| *(наименование дисциплины (модуля) в соответствии с учебным планом)* | |
| Уровень | бакалавриат, специалитет |
|  | *(бакалавриат, магистратура, специалитет)* |
| Форма обучения | очная |
|  | *(очная, очно-заочная, заочная)* |
| Направление(-я)  подготовки | 10.05.02 «Информационная безопасность» |
|  | *(код(-ы) и наименование(-я))* |
|  |  |
| Институт | Кибербезопасности и цифровых технологий |
|  | *(полное и краткое наименование)* |
| Кафедра | Информационное противоборство (КБ-8) |
|  | *(полное и краткое наименование кафедры, реализующей дисциплину (модуль))* |
| Лектор | Доцент Дедов Олег Петрович |
|  | *(сокращенно – ученая степень, ученое звание; полностью – ФИО)* |

|  |  |  |
| --- | --- | --- |
| Используются в данной редакции с учебного года | 2021/2022 | |
|  | *(учебный год цифрами)* | |
| Проверено и согласовано «\_\_\_\_» \_\_\_\_\_\_\_\_20\_\_\_г. |  |  |
|  | *(подпись директора Института/Филиала с расшифровкой)* | |

Москва 2020 г.

|  |  |  |  |
| --- | --- | --- | --- |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **МИРЭА**  Кафедра КБ-8 " Информационное противоборство " | | | |
|  | | |  |
|  | | |  |
|  | | | |
| **ЛЕКЦИЯ № 4** | | | |
| по дисциплине: | | **Б2.В,ДВ.3.1 « Криптографические методы защиты информации »** | |
|  | | (шифр и наименование учебной дисциплины) | |
| по теме: | Элементы теории чисел.Простые и составные числа. Разложение числа на множители.    Основная теорема арифметики.  Функция Эйлера и её свойства.  Теорема Ферма-Эйлера . | | |
|  | (наименование темы лекции) | | |
|  | | |
|  | | |  |
| МИРЭА – 2020 г. | | | |

Тема лекции: Элементы теории чисел. Основные определения.

Учебные и воспитательные цели:

1.Простые и составные числа. Разложение числа на множители.

2.  Основная теорема арифметики.

3.Функция Эйлера и её свойства.

4.Теоремы Ферма и Эйлера.- Ферма.

**Время:** 2 часа (90 мин.).

Литература:

а) Основная:

1. Рябко Б.Я.,Фионов А.Н. Криптография в современном мире.-М.: Горячая линия-Телеком, 2018.-300с.:ил.

2. Горбенко А.О., Основы информационной безопасности: введение в профессию.Учебное пособие, СПб: ИЦ «Интермедия», 2016.‒ 224 с.

3. Бутакова Н.Г., Федоров Н.В. Криптографические методы защиты информации. Учебное пособие, СПб: ИЦ «Интермедия», 2016. ‒ 312 с.

4.Хорев А.А., Защита информации от утечки по техническим каналам. Учебник. СПб: ИЦ «Интермедия», 2016. 920 с.

б) Дополнительная литература:

1. Зайцев А.П. и др. Технические средства и методы защиты информации. Уч. пособие. М.: Горячая линия – Телеком. 2009. – 615 с.

2. Романец Ю.В. и др. Защита информации в компьютерных системах и сетях. М.: Радио и связь. 1999. – 376 с.

3. Лозовецкий В.В. Информационная безопасность. М.: Изд. ИУИ. 2011. – 169 с.

Учебно-материальное обеспечение:

Наглядные пособия.

Технические средства обучения: проектор.

Приложения: рисунки, таблицы, слайды.

ПЛАН ЛЕКЦИИ:

**Введение** – до 5 мин.

**Основная часть** (учебные вопросы) – до 80 мин.

1.Простые и составные числа. Разложение числа на множители.-15 мин.

2.  Основная теорема арифметики 15 мин.

3.Функция Эйлера и её свойства. 15 мин.

4. Теоремы Ферма и Эйлера.- Ферма.. 20 мин.

5.Решето Эратосфена -5 мин.

Заключение – до 5 мин.

Введение – до 5 мин.

Методические рекомендации:

- показать актуальность темы;

- довести целевую установку через основные положения лекции;

- охарактеризовать место и значение данной темы в курсе;

- описать обстановку, в которой разрабатывалась теоретическая проблема и шла ее практическая реализация;

- дать обзор важнейших источников, монографий, литературы по теме;

- вскрыть особенности изучения студентами материала по рассматриваемой проблеме.

Основная часть – до 80 мин.

Введение.

**Простые и составные числа**

Каждое *натуральное число*, большее единицы, делится по крайней мере на два числа: на 1 и на само себя. Если число не имеет делителей, кроме самого себя и единицы, то оно называется **простым**, а если у числа есть еще делители, то **составным**. *Единица* же не считается ни простым числом, ни составным. Например, числа 7, 29 — простые; числа 9, 15 — составные ( 9 делится на 3, 15 делится на 3 и на 5 ).

Интересный факт: если два простых числа отличаются на 2, то их называют числами-"близнецами". Чисел-"близнецов" не очень много. Например, "близнецами" являются 5 и 7, 29 и 31, 149 и 151, а также 242 206 083\*238 880±1 (наибольшая найденная на момент написания учебного пособия пара "близнецов").

Не о всяком числе можно сразу сказать, простое оно или составное. Если число меньше ста, то, скорее всего мы сразу сможем ответить на этот вопрос. Однако с большими числами дело сложнее. Возьмем, например, число 2009. Простое оно или составное? Попробуем найти возможные делители этого числа среди первых простых чисел. 2009 определенно не делится на 2 (так как оно нечетное), на 3 (так как сумма его цифр 2+9=11 не делится на 3 ), на 5. А вот, попробовав разделить 2009 на 7, мы увидим, что в результате получается *целый* результат – 287. Таким образом, получен ответ: число 2009 – составное. В данном случае ответ получен достаточно быстро. Бывает, что проверка на простоту производится гораздо дольше, а для работы с большими целыми числами требуются даже специальные компьютерные программы.

*Поиск* больших простых чисел имеет важное *значение* для математики и не только. Например, в криптографии большие простые числа используются в алгоритмах шифрования с открытым ключом. Для обеспечения надежности шифрования там используются простые числа длиной до 1024 *бит*.

Перемножить два числа сравнительно нетрудно, особенно если у нас есть калькулятор, а числа не слишком велики. Существует и обратная задача – *задача факторизации* – нахождение двух или более чисел, дающих при перемножении заданное число. Эта задача гораздо труднее, чем перемножение чисел, и любому, кто пытался ее решить, об этом известно. Например, если от нас требуется умножить 67 на 113, то результат, 7571, будет получен, наверно, меньше чем за минуту. Если же от нас требуется найти два числа, *произведение* которых равно 7571, то, скорее всего, это займет у нас гораздо больше времени.

*Поиск* сомножителей числа n может вестись, например, перебором всех простых чисел до  как в рассмотренном выше примере с числом 2009. Однако, если множители – большие простые числа, то на их *поиск* уйдет достаточно много времени.

Таким образом, факторизация большого числа требует значительных затрат времени даже в том случае, когда известно, что оно является произведением двух больших простых чисел.

Сложность задачи факторизации используется в некоторых криптографических алгоритмах, например, в системе шифрования *RSA*.

**Основная теорема арифметики**

Любое составное число можно составить из некоторого количества простых с помощью умножения. Например, составное число 2009 можно получить так:

2009 = 7 \* 7 \* 41

В математике рассматривается так называемая **основная теорема арифметики**, которая утверждает, что любое *натуральное число* ( n>1 ) либо само является простым, либо может быть разложено на *произведение* простых делителей, причем единственным способом (если не обращать внимания на порядок следования сомножителей).

Воспользовавшись обозначением степени, разложение числа 2009 на простые множители можно записать так:

2009 = 72 \* 41

Разложение на множители называется **каноническим**, если все множители являются простыми и записаны в порядке возрастания.

Например, запишем *каноническое разложение* числа 150 на множители:

150 = 2 \* 3 \* 52

**Взаимно простые числа и функция Эйлера**

Два числа называются взаимно простыми, если они не имеют ни одного общего делителя кроме единицы.

Например, числа 11 и 12 взаимно просты (у них нет общих делителей кроме единицы), числа 30 и 35 — нет (у них есть общий делитель 5 ).

Исследованием закономерностей, связанных с целыми числами, долго занимался швейцарский математик Леонард Эйлер (Leonard Euler). Одним из вопросов, которым он интересовался, был следующий: **сколько существует натуральных чисел, не превосходящих n и взаимно простых с n?** Ответ на этот вопрос был получен Эйлером в 1763 году и этот ответ связан с каноническим разложением числа n на простые множители. Так, если



где p1, p2, ..., pn – разные простые множители, то число  натуральных чисел, не превосходящих n и взаимно простых с n можно точно определить по формуле



Число натуральных чисел, не превосходящих n и, взаимно простых с n, называется **функцией Эйлера** и обозначается 

Например, найдем количество натуральных чисел, не превосходящих 12 и взаимно простых с 12. Из ряда натуральных чисел

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

взаимно простыми (не имеющими общих делителей) с 12 будут только числа 1, 5, 7, 11. Их количество равно четырем. Таким образом 

Теперь попробуем подсчитать



по формуле, предложенной Эйлером. Для этого вначале запишем *каноническое разложение* числа 12:

12 = 22 \* 3.

Теперь подсчитаем функцию Эйлера :



Значения, вычисленные путем простого перебора взаимно простых чисел и по формуле Эйлера, совпали. Это неудивительно, так как формула для вычисления функции Эйлера может быть доказана строго математически.

Формулу Эйлера удобно использовать для больших n, если известно разложение числа n на простые множители. Для криптографии формула Эйлера важна тем, что она позволяет легко получить число



для простых и некоторых других чисел. В криптографии используются два следующих следствия формулы Эйлера.

**Следствие 1**. Если p – *простое число*, то 

Действительно, если p – *простое число*, то его *каноническое разложение* состоит только из него самого. Тогда



**Следствие 2**. Пусть р и q — два различных простых ( ). Тогда



Эта формула объясняется следующим образом. Пусть р \* q = N, где р и q — два различных простых (  ). Тогда



Рассмотрим несколько примеров использования следствий формулы Эйлера.

**Пример 1**. Найдем  13 – *простое число*, значит, используя следствие 1  Мы можем проверить себя (и Эйлера), выписав все числа, меньшие 13:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

и подсчитав все взаимно простые с ним. Их действительно 12.

**Пример 2**. Найдем  35 – составное число, значит, первое следствие нам не подходит. Однако 35 является произведением двух простых чисел: 35 = 5 \* 7. Используя следствие 2, вычисляем :



Проверяем, выписывая все числа, меньшие 35 и не имеющие с ним общих делителей:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

Их действительно оказалось 24. На последнем примере видно, что использовать формулу Эйлера гораздо удобнее, чем рассматривать все числа из довольно большого диапазона и проверять на взаимную простоту.

**Малая теорема Ферма**

В основе алгоритма шифрования по системе *RSA* лежит теорема, сформулированная в начале семнадцатого столетия без доказательства французским математиком Пьером Ферма (Pierre Fermat). Её часто называют "Малой *теоремой Ферма*", и её не следует путать с известной "Великой *теоремой Ферма*" - её он также сформулировал без доказательства, а доказана она была только в 1993-94 годах. Леонард Эйлер в 1760 году опубликовал *доказательство* Малой теоремы Ферма и получил ее *обобщение*, известное под названием теоремы Ферма-Эйлера. Именно эта теорема используется в алгоритме зашифрования/расшифрования *RSA*.

**Малая теорема Ферма** формулируется следующим образом. Если p - *простое число*, а m - любое число, которое не делится на p, то



то есть число mp-1 при делении на p дает *остаток* 1.

Например, пусть р=11, m = 3. Проверим, будет ли 310 mod 11 равно одному:

310 mod 11=32( ((32)2)2mod 11)) = 9(42 mod 11 )= 144 mod 11=1

**Возведение a в степень b по модулю 7.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **a\b** | **1** | **2** | **3** | **4** | **5** | **6** |
| **1** | **1** | **1** | **1** | **1** | **1** | **1** |
| **2** | **2** | **4** | **1** | **2** | **4** | **1** |
| **3** | **3** | **2** | **6** | **4** | **5** | **1** |
| **4** | **4** | **2** | **1** | **4** | **2** | **1** |
| **5** | **5** | **4** | **6** | **2** | **3** | **1** |
| **6** | **6** | **1** | **6** | **1** | **6** | **1** |

**Остатки от деления на 7 шестой степени(1,2,3,4,5,6):**

**16**=1=0\*7 +1

2**6=64=9\*7 +1**

**36=729=104\*7+1**

**46= 4096= 585\*7+ 1**

**56=15625= 2232\*7 +1**

**66=46656= 6665\*7+1**[[1]](#endnote-2)

*Обобщение*, сформулированное и доказанное Эйлером, справедливо для любого модуля, но в системе *RSA* используется частный случай, когда *модуль* является произведением только двух различных простых чисел. Поэтому рассмотрим формулировку теоремы для этого случая.

**Теорема Эйлера: Пусть а и b взаимно простые числа.**

**Тогда а(^(ϕ(b)) modb =1**

Например, если модуль =12, то функция Эйлера будет равна 4 и для оснований a =5 и a=2( второй пример) мы получим, что результат= 1, проверим это

То есть, вычислим а в степени Ф (b) mod b и убедимся, что результат для разных значений а =1.

Пример :

1). Ф (12) = 4; отсюда следует, что для а=5

5 в 4-ой степени по mod 12 = 625 mod 12=1.

5 Ф (12) mod12=1.

2) Ф ( 21) = 2\*6=12; отсюда следует, что для а=2

2 в 12-ой степени по mod 21 = 16(^ 4) mod 21=1.

2Ф (21) mod 21=1.

**Теорема Ферма-Эйлера** (для случая системы *RSA*). Если p и q - два различных простых числа, а m - любое число, которое не делится на p и q, то



Например, пусть р=11, q = 5 (pq = 55), m = 3. Проверим, будет ли 340



равно одному:

340 mod 55 = (35) 8mod 55 = 234 mod 55 = 279841 mod 55 = 1.

3(^5)=243 23(^2)=529---34(^2)= 1156 1

**Инверсия по модулю m**

Во многих задачах криптографии для заданных чисел с, m требуется находить такое число d < m, что

cd mod m = 1

Такое d существует тогда и только тогда, когда числа с и m взаимно простые. Число d, удовлетворяющее равенству cd mod m = 1, называется **инверсией** с **по модулю** m и часто обозначается с-1 mod m. Данное обозначение для инверсии связано с тем, что *равенство* cd mod m = 1 можно переписать в виде

cс-1 mod m = 1.

Таким образом, *умножение* на с-1 соответствует делению на с при вычислениях по модулю m.

Инверсию по модулю m также можно вычислять с помощью обобщенного алгоритма Евклида.

Покажем, как это делается. *Равенство*, приведенное ниже означает, что для некоторого целого k имеет *место* *равенство* cd – km = 1. Учитывая, что с и d взаимно просты, можно преобразовать это *равенство* следующим образом:

m(-k) + cd = НОД(m,c).

Значит, мы можем вычислить с-1 mod m (или найти число d ) с помощью обобщенного алгоритма Евклида. При этом *значение* переменной k нас не интересует. Если число d получается отрицательным, то нужно прибавить к нему m, так как по определению число a mod m берется из *множества* {0,1,..., m - 1}.

Вычислить НОД( 1067, 427) , инверсию иs1, t1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | q | r1 | r2 | r | s1 | s2 | s | t1 | t2 | t |
| 1 | 2 | 1067 | 427 | 213 | 1 | 0 | 1 | 0 | 1 | -2 |
| 2 | 2 | 427 | 213 | 1 | 0 | 1 | -2 | 1 | -2 | 5 |
| 3 | 213 | 213 | 1 | 0 | 1 | -2 | 427 | -2 | 5 | -1067 |
|  |  | 1 |  |  | -2 |  |  | 5 |  |  |

-2\*1067 +5\*427=1

Вычислить НОД( 1001,73 ) , инверсию-t1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | q | r1 | r2 | r | t1 | t2 | t |
| 1 | 13 | 1001 | 73 | 52 | 0 | 1 | -13 |
| 2 | 1 | 73 | 52 | 21 | 1 | -13 | 14 |
| 3 | 2 | 52 | 21 | 10 | -13 | 14 | -41 |
| 4 | 2 | 21 | 10 | 1 | 14 | -41 | 96 |
| 5 | 10 | 10 | 1 | 0 | -41 | 96 | -1001 |
|  |  | 1 |  |  | 96 |  |  |

96\*73=7008; 7008 - 7\*1001=1.

Таким образом, получили, что 73-1 mod 1001 = 96. Проверим: 73\*96 mod 1001 =1.

**Решето Эратосфена**

Греческий математик Эратосфен изобрел метод, как найти все простые числа, меньшие, чем n.

Метод назван **решетом Эратосфена.**Предположим, что мы хотим найти все числа, меньшие, чем 100. Мы записываем все числа между 2 и 100. Поскольку \sqrt 100  = 10, мы должны видеть, делим ли без остатка любой номер меньше чем 100 на числа 2, 3, 5 и 7. [Таблица 2.1](https://www.intuit.ru/studies/curriculums/4081/courses/408/lecture/9368?page=1#table.12.1) показывает результат.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица 2.1. *Решето Эратосфена* | | | | | | | | | |
|  | **2** | **3** | 4 | **5** | 6 | **7** | 8 | 9 | 10 |
| **11** | 12 | **13** | 14 | 15 | 16 | **17** | 18 | **19** | 20 |
| 21 | 22 | **23** | 24 | 25 | 26 | 27 | 28 | **29** | 30 |
| **31** | 32 | 33 | 34 | 35 | 36 | **37** | 38 | 39 | 40 |
| **41** | 42 | **43** | 44 | 45 | 46 | **47** | 48 | 49 | 50 |
| 51 | 52 | **53** | 54 | 55 | 56 | 57 | 58 | **59** | 60 |
| **61** | 62 | 63 | 64 | 65 | 66 | **67** | 68 | 69 | 70 |
| **71** | 72 | **73** | 74 | 75 | 76 | 77 | 78 | **79** | 80 |
| 81 | 82 | **83** | 84 | 85 | 86 | 87 | 88 | **89** | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | **97** | 98 | 99 | 100 |

Процесс состоит в следующем:

1. Вычеркнуть все числа, *делимые* без остатка на 2 (кроме самого 2).
2. Вычеркнуть все числа, *делимые* без остатка на 3 (кроме самого 3).
3. Вычеркнуть все числа, *делимые* без остатка на 5 (кроме самого 5).
4. Вычеркнуть все числа, *делимые* без остатка на 7 (кроме самого 7).
5. Оставшиеся числа – простые.

**Ключевые термины**

**Алгоритм Евклида** – математический *алгоритм*, который может использоваться для нахождения наибольшего общего делителя двух чисел.

**Взаимно простые числа** – числа, не имеющие общих делителей (кроме единицы).

**Задача факторизации** – нахождение двух или более натуральных чисел, дающих при перемножении заданное число.

**Инверсия по модулю** – такое *натуральное число*, которое при умножении по модулю на данное число дает в результате единицу.

**Каноническое разложение на множители** – такое разложение на множители, при котором все множители являются простыми и записаны в порядке возрастания.

**Малая теорема Ферма** – известная теорема, сформулированная П. Ферма, лежащая в основе алгоритма шифрования по системе *RSA*

**Наибольший общий делитель** чисел а и b – наибольшее число с, которое делит и а и b: с = НОД(a, b).

**Основная теорема арифметики** – теорема утверждающая, что любое *натуральное число* большее единицы либо само является простым, либо может быть разложено на *произведение* простых делителей, причем единственным способом (если не обращать внимания на порядок следования сомножителей).

**Простое число** – *натуральное число*, которое не имеет делителей, кроме самого себя и единицы.

**Составное число** – *натуральное число*, которое делится, помимо самого себя и единицы, еще хотя бы на одно число.

**Функция Эйлера** позволяет подсчитать число натуральных чисел, не превосходящих n и, взаимно простых с n. Обозначается

**Рациональные числа:-целые(…. -2, -1, 0,1, 2, 3…..)**

**-дробные( -3\2= -1,5 ; 1\7=0,142857…)-отношение в виде двух целых чисел или в виде десятичной дроби: конечной или бесконечной периодической.**

**Целые числа – натуральные, ноль и отрицательные( ….-2 ,-1, 0, 1, 2, 3….). Натуральные -целые числа не меньше единицы 1, 2, 3, ….**

**-неотрицательные целые числа 0, 1, 2, 3…..**

**Отдельный класс –иррациональные числа – Пи, корень квадратный, ехр ….**

**Простые числа от 2 до 20:- 2,3, 5,7,11,13,17,19.**

**Разложение составного числа на множители**

**4= 2\*2**

**6=2\*3**

**8=2\*2\*2**

**9=3\*3**

**10=2\*5**

**12=2\*2\*3**

**14=2\*7**

**15=3\*5**

**16=2\*2\*2\*2**

**18=2\*3\*3**

**20=2\*2\*5**

**Если натуральное число N не делится без остатка ни на одно из простых чисел, которые меньше или равны корню квадратному из N, то это число простое.**

**Решето Эратосфена для больших чисел – сложно. Отсюда тест Ферма:**

**Тест Ферма- если для любого целого числа а , которое не делится на n, выполняется сравнение a в степени n-1 сравнимо с 1 по (modn), то оно простое. Число Кармайка 561 не является простым Тест Миллера – Рабина в 4 раза точнее Ферма.**

**Разложение на простые множители просто только для небольших чисел(см. выше).**

**Для разложения числа 1001 применяем формулу x3+ y3=(x+y)(x2-xy+y2)**

**Представим 1001= 103 + 13= (10+1)(100-10+1)= 11\*91= 78\*11\*13.**

**Для числа 9991 применяем x2-y2 =(x+y)(x-y). 9991= 1002 – 3 2 = (100+3)(100-3)= 103\*97.**

**Для числа 10001 перебираем по одному все простые числа меньше или равные Корень квадратный из 10001 --- 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97.**

**В результате 10001= 73\*13**

1. [↑](#endnote-ref-2)